Title	Carlitz加群と整数環のGalois加群構造(群スキームの変形と整数論への応用)
Author(s)	相羽, 明
Citation	数理解析研究所講究録 (1996), 942: 134-141
Issue Date	1996-04
URL	http://hdl.handle.net/2433/60150
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
942巻 1996年 134-141

Carlitz 加群と整数環の Galois 加群構造

茨城大理　相羽　明　（ AKIRA AIBA ）

§1. 序

$K/\mathbf{Q}$:有限次拡大、N/K:Galois拡大、$G=Gal(N/K)$ を Galois群とします。この時

N/Kが正規整数底 (normal integral basis 以下 n.i.b. と略す) をもつとは、

「O_N(Nの整数環)の元αが存在して $\{\alpha^\sigma\}_{\sigma\in G}$が O_Nの O_K上自由基底となる」

と定義します。

これを、あとで拡張する際便利なように群環の言葉で表すと

「O_Nは O_Nの元αを自由基底とする rank 1 の $O_K[G]$-自由加群である」となります。また上のαを n.i.b. の生成元と呼びます。

この時 N/Kはいつ n.i.b. を持つか？　また持つとき n.i.b. の生成元を具体的に与えよ、という問題を考えます。(もちろん今まで述べたことは Kが代数体でなくとも”整数環”が存在すれば同じように定義し問題を立てることが出来ます。実際、2節以降で取り扱う Kは一変数有理関数体で、対応する問題を考えます。)この問題は Galois拡大における正規底定理から自然にでてくるものであり、また河本氏の講演その他にありましたように多くの応用があります。

これについて最も基本的な結果は、

HILBERT-SPEISER. $N/\mathbf{Q}$:有限次 abel拡大で高々tame に分岐ならば n.i.b. を持ち、n.i.b. の生成元も具体的に求まる。

です。

例. $n = p_1 \dots p_s$、但し p_i $(i = 1, \cdots, s)$ は相異なる素数とする。ζ_nを 1 の原始 n 乗根とする。この時 $N = \mathbf{Q}(\zeta_n)$ ならば、ζ_nが n.i.b. の生成元となる。

N/Kが n.i.b. を持つには N/Kが高々 tame に分岐の拡大であることが必要であることが知られていますので (例えば[4]定理 3)、このままの形では Hilbert-Speiser の定理は wild な分岐を含む abel 拡大へ拡張できません。そこでどうするか。いろいろなやり方が考えられるでしょうが、Leopoldt は次に定義する $A(N/K)$ を使ってうまく Hilbert-Speiser の定理を拡張しました。

$$A(N/K) := \{\lambda \in K[G]; \lambda O_N \subset O_N\} \supset O_K[G]$$

LEOPOLDT [6] ([7]も参照). $N/\mathbf{Q}$:有限次 abel 拡大ならば、O_Nは rank 1 $O_K[G]$-自由加群。自由基底も具体的に求まる。

注) $\phi \in \hat{G}$(指標群) に対して、$e_\phi = \frac{1}{\#G} \sum_{\gamma \in G} \phi(\gamma^{-1})\gamma$を対応する巾等元、 $f(\phi)$ を導手とします。 $f_t(\phi) = \prod_{\substack{\ell \| f(\phi) \\ \ell:\text{素数}}} \ell$ を導手の tame-part 、 $f_w(\phi) = f(\phi) f_t(\phi)^{-1}$を wild-part とします。 $\hat{G}$の元χ, ϕに

$$\chi \sim \phi \Longleftrightarrow f_w(\chi) = f_w(\phi)$$

と同値関係を入れ、$\Phi \in \hat{G}/\sim$に対して $e_\Phi = \sum_{\phi \in \Phi} e_\phi$と置きます。この時 Leopoldt は更に

$$A(N/\mathbf{Q}) = \sum_{\Phi \in \hat{G}/\sim} e_\Phi \mathbf{Z}[G]$$

ということも示しました。($N/\mathbf{Q}$ が tame の時、$A(N/\mathbf{Q}) = \mathbf{Z}[G]$になっていることに注意)

例. $n = p_1^{e_1} \cdots p_s^{e_s}$ 但し p_iは相異なる素数で e_iを自然数 $(i = 1, \ldots, s)$ とする。この時 $N = \mathbf{Q}(\zeta_n)$ ならば、$\alpha = \prod_{i=1}^{s} (\sum_{a_i=1}^{e_i} \zeta_{p_i}^{a_i})$ が自由基底となる。

上記二定理の証明はもちろん大きく Kronecker-Weber の定理に依存しています。一方すでに他のいくつかの拡大において Kronecker-Weber の定理の類似定理が知られています。これら類似定理のある場合に上記二定理にあたるものはあるのだろうか、という疑問が浮かんで来ます。この小文では次節以降特に有理数体のかわりに、有限体上一変数有理関数体で考えた場合どうなるかについて述べていきます。

§2. Carlitz 加群の復習

本節では有限体上一変数有理関数体での Kronecker-Weber の類似定理を復習します。(詳しくは[5]または[2]を参照して下さい。) まずいくつかの記号を導入し、定理の記述に必要な Carlitz 加群を定義します。

以下 q : p-巾 (p は素数) を固定します。(主定理では qは奇数と制限します。) $k = \mathbf{F}_q$を位数 qの有限体、$k_n = \mathbf{F}_{q^n}$、$K = k(T)$、$K_n = k_n(T)$、$O = O_K = k[T]$ とします。

定義. $M \in O$に対して、$[M] \in O[X]$を以下のように決める。

(1) $[1] = X$

(2) $[T] = X^q + TX$

(3) $[T^n] = [T] \circ [T^{n-1}]$ ($\circ$ は合成関数)

(4) $M(T) = \sum a_i T^i$ $(a_i \in k)$ ならば $[M] = \sum a_i [T^i]$

この $M \in O$から$[M] \in O[X]$への写像を Carlitz 加群と呼びます。

Carlitz 加群を使って$\Lambda_M := \{x \in K^{ac}; [M](x) = 0\}$ (但し K^{ac}は Kの代数閉包) と定義するとΛ_Mは Kの分離閉包に入り、[ ]の積により O/MO加群となります。λ_MをΛ_Mの自由基底とします。このΛ_Mが有理数体での 1 のm乗根全体、λ_Mが 1 の原始m乗根に対応します。

すると $K_M := K(\Lambda_M)$が円分体に対応してなければなりませんが実際次のように Galois 群の構造や分岐についてよく似た性質を持っています。

◇ K_M/Kは Galois(abel) 拡大で次の写像は同型、

$$(O_K/MO_K)^* \ni N \longmapsto \sigma_N \in Gal(K(\Lambda_M)/K)$$

但し$\sigma_N(\lambda_M) = [N](\lambda_M)$です。

◇ $P \in O$ を既約とすると、拡大 K_{P^r}/K (rは自然数) は素イデアル PO上完全分岐、それ以外の素イデアル上不分岐。

今の場合無限素点についても考慮しなければなりませんのでそれについていくつか記号を導入します。

$O'_K := k[1/T] \subset K$と置き、$M \in O'_K$に対して$[M]' \in O'_K[X]$を$[1/T]' = X^q + (1/T)X$であとは[ ]と同様に定義します。$\Lambda'_n := \{x \in K^{ac}; [T^{-n-1}]'(x) = 0\}$として、$L_n$を $K(\Lambda'_n)$ の k^*での固定体とします。

これで Kronecker-Weber の類似定理を述べるための準備が出来ました。

定理. N/Kを有限次 abel 拡大ならば、monic な多項式 $M \in O_K$と $m \geq 1$, $n \geq 0$ なる整数が存在して、

$$N \subset k_n(T) \cdot K_M \cdot L_m$$

となる。

特に N/Kが O_Kの素イデアルで高々tameに分岐の abel拡大ならば、monic で square-freeの多項式 $M \in O_K$と $m \geq 1, n \geq 0$なる整数が存在して、

$$N \subset k_n(T) \cdot K_M \cdot L_m$$

となる。

§3.§1の結果の関数体での類似

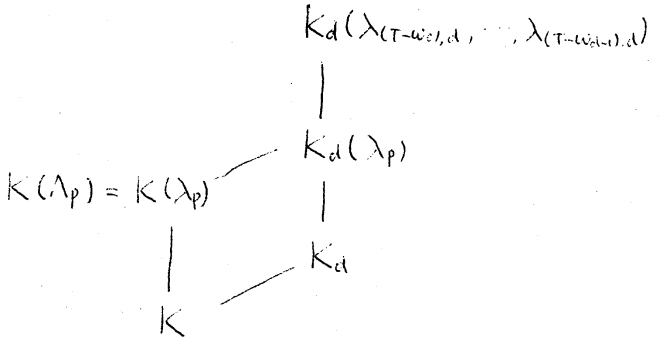
§2の結果を使って Chapmanは Hilbert-Speiserの定理の類似を証明しました。

CHAPMAN[2]. N/Kが O_Kの素イデアルで高々tameに分岐の abel拡大で、O_Nが O_Kの Nにおける整閉包（Nの整数環）ならば、O_Nは rank 1の自由 $O_K[G]$-加群で自由基底も具体的に求まる。いいかえると N/Kは n.i.b.を持ち、n.i.b.の生成元も具体的に求まる。

例. $P \in O_K$ monic既約な多項式の時

$$\alpha = \sum_{k=0}^{q^d-1} \prod_{j=0}^{d-1} \lambda_{(T-\omega_j),d}^{<kq^{d-j-1}>}$$

が $K(\Lambda_P)/K$の n.i.b.の生成元。ここで dは Pの次数、$P = \prod(T-\omega_j)$、$\omega_j \in k_d^\star$ を$\omega_j^q = \omega_{j+1}$のようにとる $(j = 0, \cdots, d-1)$。$\lambda_{(T-\omega_j),d}$は基礎体を kでなく k_dとしてλ_Mと同様に定義したもの。 $<\ >$は mod q^d-1で最小の正の数 とする。



証明は直接計算しようとすると次数が2以上の既約多項式のところが大変に

なります。そこで例に挙げた場合で説明すると、まず基礎体 k を k_d まであげて $k_d(\Lambda_{(T-\omega_1),d},\cdots,\Lambda_{(T-\omega_d),d})/k_d$の n.i.b. を求め、そして $k(\Lambda_P)/k$へ落とすというやり方で示されています。次に Leopoldt の定理の類似はどうなっているかという疑問が浮かびます。それについて以下の結果が示せました。

主定理. qを奇素数巾、$P\in O$を次数 1 の多項式、 $N=K(\Lambda_{P^2})$ ならば O_N は自由 $A(N/K)$ 加群ではない。

§4. 主定理の証明のあらすじ

当分の間 q は必ずしも奇でない素数巾、Pの次数は任意で、P^2の代わりに P^n（ n は任意の自然数）で考えます。

補題 1 . O_Nが $A(N/K)$-加群として自由ならば、$\alpha\in O_N$が自由基底であるための必要十分条件は任意の$\beta\in O_N$に対して$\det(\alpha^{\sigma\tau})_{\sigma,\tau\in G}$ が$\det(\beta^{\sigma\tau})_{\sigma,\tau\in G}$を割り切ることである。

補題 1 から$\det(\alpha^{\sigma\tau^{-1}})$ $(\alpha\in O_N)$ の計算が重要になります。そのため次の群行列式の公式（有名な巡回行列式の公式の一般型）の正標数版を使います。

補題 2 . pを素数、$G=G_0\times G_1$を有限次 abel 群（但し G_0は G の p-シロー部分群）とする。更に、fをある標数 p の体に値を持つ G 上の関数とするならば

$$\det(f(\sigma\tau^{-1}))_{\sigma,\tau\in G}=\prod_{\chi\in\hat{G}_1}\Big(\sum_{\tau\in G_0}\Big(\sum_{\sigma\in G_1}\chi(\sigma)\Big)f(\sigma\tau)\Big)^{\#G_0}$$

補題 2 を

$$G=Gal(K(\Lambda_{P^n})/K)\simeq Gal(K(\Lambda_{P^n})/K(\Lambda_P))\times Gal(K(\Lambda_P)/K)$$

に適用すると$\det(\alpha^{\sigma\tau^{-1}})_{\sigma,\tau}$は、$\prod_{\chi}(\sum_{\sigma}\chi(\sigma)\,\mathrm{Tr}_{K(\Lambda_{P^n})/K(\Lambda_P)}\,\alpha)^{\sigma})^{q^{n-1}}$ となり、行列式の計算は$\mathrm{Tr}_{K(\Lambda_{P^n})/K(\Lambda_P)}(\lambda_{P^n}^{i})$ $(0\leq i<q^n-q^{n-1})$ に帰着されます。ここで計算の都合上 Pの次数を 1 に仮定します。すると次の Newton の公式:

補題 3. $\alpha_1,\cdots,\alpha_t$ を任意の数、

$$s_1=\alpha_1+\alpha_2+\cdots+\alpha_t$$

$$s_2=\alpha_1\alpha_2+\alpha_1\alpha_3+\cdots+\alpha_{t-1}\alpha_t$$

$$\vdots$$

$$s_t=\alpha_1\alpha_2\cdots\alpha_t$$

を基本対称式、

$$\sigma_n=\alpha_1^n+\alpha_2^n+\cdots+\alpha_t^n$$

とするならば

$$\sigma_n=\begin{cases}\sum_{i=1}^{n-1}(-1)^{i+1}\sigma_{n-i}s_i+(-1)^{n+1}ns_n & \text{if } n\leq t \quad (1)\\ \sum_{i=1}^{t}(-1)^{i+1}\sigma_{n-i}s_i & \text{if } n>t \quad (2)\end{cases}$$

をλ_{P^n}の $K(\Lambda_P)$ 上の最小多項式$[P^{n-1}](X)-\lambda_P$に使うと、任意の $K(\Lambda_{P^n})$ の元αに対して$\det(\alpha^{\sigma\tau^{-1}})$ はすべて $d:=P^{\frac{q^{n-1}(q-2)}{2}+(n-1)(q-1)q^{n-1}}$を割り切ることがわかります。また例えば$\eta:=\sum_{A=0}^{q-2}\lambda_{P^n}^{q^{n-1}-1+Aq^{n-1}}$とおけば$\det(\eta^{\sigma\tau^{-1}})$になります。

注). $O_{K(\Lambda_{P^n})}$は $O[\lambda_{P^n}]$と等しくその判別式が $P^{q^{n-1}(nq-n-1)}$になることが知られています (c.f.[5])。上の判別式と d^2の P-巾の差は $q^{n-1}(q-1)(n-1)$ となります。

補題 1 より$\sigma(\eta)\in O_N$なる$\sigma\in K[G]$が $A(N/K)$ の元か調べてやれば O_Nが自由 $A(N/K)$-加群かどうかわかります。計算の都合上 $n=2$,q を奇素数巾とし

ます。すると実際 $\rho := P^{\frac{q-3}{2}} \sum_{a,b} b^{\frac{q-1}{2}} \sigma_{aP+b} + (-1)^{\frac{q+1}{2}} \frac{1}{P} \sum_{a,b} a^{\frac{q-1}{2}} \sigma_{aP+b}$ と置くと、 $\rho(\eta) = \lambda_{P^2}^{\frac{q-1}{2}}$ は O_N の元ですが、$\rho(\lambda_{P^2}^{(q-1)/2}) = (-1)^{(q+1)/2} \lambda_P^{(q-1)/2}/P$ は O_N にはいりませんので $\rho \notin A(N/K)$ となり自由加群でないことが証明されます。

§5. 最後に

円分体の整数環の Galois 加群構造について §1 の結果の他に Chan と Lim の結果 [3]（[1]も参照）があります。これについても §3 のやり方が使えます。

参考文献

[1] W.Bley, A Leopoldt-type result for rings of integers of cyclotomic extensions, Canad. Math. Bull. **38** (1995), 141–148.

[2] R.J.Chapman, Carlitz modules and normal integral bases, J. London Math. Soc. **44** (1991), 250–260.

[3] S.P.Chan and C.H.Lim, Relative Galois module structure of rings of integers of cyclotomic fields, J. Reine Angew. Math. **434** (1993), 205–220.

[4] A.Fröhlich, Galois module structure of algebraic integers, Springer, 1983.

[5] D.R.Hayes, Explicite class field theory for rational function fields, Trans. Amer. Math. Soc. **189** (1974), 77–91.

[6] H.-W. Leopoldt, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. Reine Angew. Math. **201** (1959), 119–149.

[7] G.Lettl, The ring of integers of an abelian number field, J. Reine Angew. Math **404** (1990), 162–170.